Approved For Release 2007/07/10 : CIA-RDP86B00689R000300070005-6

SECRET

Working Group V

Information Protection & Management

1. Summary and Conclusions

2. Security

   a. Policy

   b. Hardware and Technology Impact

   c. Disks and Terminal Management

   d. Personnel and Physical Security Standards

   e. Dissemination Control and Compartmentation

   f. Other Security Issues

   g. Security Goals and Objectives

3. Information Management

   a. Records Management

   b. Administration

   c. Control, Storage and Archiving

   d. Data Definition Standards

   e. Goals and Objectives

Approved For Release 2007/07/10 : CIA-RDP86B00689R000300070005-6

Approved For Release 2007/07/10 : CIA-RDP86B00689R000300070005-6

1. Summary and Conclusions

IHSA Working Group V met on 23 and 24 November 1981 to review the IHSA point paper on Information Protection and Management and discuss other issues relevant to this general area of interest. The objective of these two sessions was to collectively determine and propose the direction the Agency should pursue in the formulation of Security and Information Management strategic goals for the 1985-1989 timeframe. The Group concluded that there is a definite need for 1) establishment of unambigious security policy concerning Information Handling Systems, 2) judicious selection and attention to technological advances and their application to security safeguards and 3) generating authoritative directives to guide and enforce records management procedures. Based on these holistic conclusions, the group opined that a framework existed from which achievable goals could be formulated to focus IHSA efforts in Strategic Planning.

2. Security

a. Policy

DCID 1/16 and [redacted] provide existing security guidelines and policy regarding ADP systems. It was the consensus of the Working Group that they do not adequately cover or reflect the current ADP environment nor will they be applicable in the 1985-1989 timeframe. The dynamics involved in Information Handling systems make it difficult for users to find comfort in their adherence to current security policy and guidelines. It was recommended that security policy be promulgated which better defines the aspects of IHS's, and that more explicit responsibilities for adherence to

25X1

Approved For Release 2007/07/10 : CIA-RDP86B00689R000300070005-6

Approved For Release 2007/07/10 : CIA-RDP86B00689R000300070005-6

25X1

security practices and procedures be established. A rewrite of [redacted] and DCID 1/16 is specifically recommended to incorporate current and future policies regarding security. Moreover, security policy should be a major consideration in new system design and development.

b. Hardware and Technology Impact

Technology is developing and becoming available which can greatly enhance ADP system security. This is especially true in the areas of automated dissemination controls, to aid in maintaining compartmentation, secure operating systems, and encryption of data bases. Extension of large data bases such as envisioned in SAFE to NFIB membership must incorporate protective measures against the unauthorized or accidental disclosure of sensitive, compartmented information. Connectivity to and interoperability with the Intelligence Community must not, therefore, be accomplished in the System high mode.

It was also recommended that reliability requirements for IHS hardware be developed to include exhaustive Single Failure Analysis and Security Fault Analysis documentation. As the U.S. Government now commands only approximately ten percent of the computer market, these specifications, may, in many cases, be difficult to comply with. However, this is considered more cost-effective than to retrofit available commercial hardware with security safeguards.

Approved For Release 2007/07/10 : CIA-RDP86B00689R000300070005-6

Approved For Release 2007/07/10 : CIA-RDP86B00689R000300070005-6

c. Disks and Terminal Management

Local storage of data in either hard disks, floppys or terminal memories was not considered a problem as technology (i.e., laser disks, etc.) is providing alternate and acceptable methods which will meet our present concerns in the 1985-9 timeframe. Floppys were considered individual tools for temporary, local use, much as mag cards. It was concluded that we need not formulate long range plans for these devices except for security controls to prevent unauthorized removal from Agency premises. Technology is moving fast toward greater storage density on hard disks. Hard disks are to be located in centers meeting vault specifications.

The Committee agreed that ODP must assure through proper controls that data will not be left in the Delta Data standard terminal's memory during unattended periods.

d. Personnel and Physical Security Standards

Personnel are our most important asset, and a sound personnel security program is of foremost importance. There should be more frequent security reinvestigations on the one hand and more careful treatment of our personnel on the other.

The Group opined that technical, personal and physical security standards will remain major considerations in the development, procurement and deployment of future IH systems. Continuing awareness of threats, vulnerabilities and opportunities will be required to keep pace with technological developments. Careful screening of prospective employees, coupled with ongoing reinvestigations of career employees, will also

Approved For Release 2007/07/10 : CIA-RDP86B00689R000300070005-6

Approved For Release 2007/07/10 : CIA-RDP86B00689R000300070005-6

continue as a minimum requirement for access to and operation of Information Handling systems and data bases.

e. Dissemination Control and Compartmentation

Automatic dissemination control is becoming available with today's technology. New technological initiatives should be pursued with budgetary backing to bring automatic dissemination into the Agency.

It can also be assumed that future operational environments will require that access to Agency data bases be extended to non-CIA entities and to overseas locations. Furthermore, access limitations, compartmentation and ever increasing requirements for accountability and audit trails will place additional tasking on our already limited resources. Improved formats and scrutiny of audit trails are required.

The Committee identified SAFE as the system most likely to require special compartmented security precautions, due to its contemplated access by the Intelligence Community. The Committee expressed the opinion that networking, connectivity, and interoperability must not necessarily be regarded as goals in themselves in an intelligence environment, as they create serious security hazards. Essential compartmentation may need to be achieved by discouraging interoperability.

CRAFT managers assert that direct field access of Headquarters data bases is unlikely to be implemented to any significant degree by the CRAFT program until after the 1985-1989 period. Regardless of when it comes, this will certainly pose a significant security challenge for Information managers. Alternatives to the use of shielded enclosures should be sought for the CRAFT project overseas to enable terminals to be used on individual officers' desks.

Approved For Release 2007/07/10 : CIA-RDP86B00689R000300070005-6

Approved For Release 2007/07/10 : CIA-RDP86B00689R000300070005-6

f. Other Security Issues

A major problem in NFAC is the need to rationalize compartmentation so that analysts will have access to needed intelligence information. Compartmentation of operational information in the DO and the S&T must continue to receive emphasis. Greater dispersion of computer data bases should be anticipated in the 1985-1989 timeframe; their networking or isolation will become ever more an issue, with all of the security ramifications entailed.

Lastly, although another Agency committee is considering the issue of foreign procurement of ADP equipment, there was some sentiment in the Group for new policies which make all Agency ADP procurements classified and give less emphasis to competitive procurements. These measures could reduce our security vulnerability and increase our industrial clout in the procurement process.

g. Security Goals and Objectives

To ensure optimum protection for our information, the Working Group submits the following goal as a statement of Agency efforts in planning for an Information Handling Systems Architecture:

> Promulgate security policy and guidelines which more precisely define areas of responsibilities, assign accountability, identify authority and encourage judicious application of technology for the protection of information in the future IH environment.

In pursuit of this goal, the following objectives are proposed:

Approved For Release 2007/07/10 : CIA-RDP86B00689R000300070005-6

Approved For Release 2007/07/10 : CIA-RDP86B00689R000300070005-6

Objective 1.1: Review and rewrite, where applicable and as appropriate, [redacted] and DCID 1/16.

25X1

Objective 1.2: Develop an acceptable and reliable emergency destruction technique for digitally stored data.

Objective 1.3: Explore technology to identify new devices, techniques or methodologies for application in dissemination controls, access limitations, compartmentation, and emanations control.

Objective 1.4: Incorporate security enhancements into system design and procurement which will accomplish security policy, for audit trails in particular.

Objective 1.5: Continue research in secure operating systems for information protection through encrypted data bases.

Objective 1.6: Expand current security policy to specify more frequent reinvestigations for ADP personnel.

Approved For Release 2007/07/10 : CIA-RDP86B00689R000300070005-6

Approved For Release 2007/07/10 : CIA-RDP86B00689R000300070005-6

3. Information Management

a. Records Management

National Archives and Records Service (NARS) guidance on records management is outdated. The transition of information from paper to electronic form has essentially outstripped the applicability of existing NARS regulations on records control schedules and records management. The basic issue of what constitutes a temporary and what constitutes a permanent record continues to be a major problem. Electronic data storage techniques have further exacerbated the problem by combining the storage of information in data bases containing both temporary and permanent records. The labor-intensiveness of managing data bases and purging temporary from permanent records lessens the incentive to do so. The lack of resources to dedicate for this purpose results in delegating a very low priority to this records management function.

b. Administration

The Office of Information Services (OIS), Records Management Division provides guidance to the Agency on records management issues and is also the focal point for NARS. Records Management Officers (RMO's) in Agency components perform an advisory role on records management except in the Directorate of Operations where the RMOs have staff management responsibility for the DO information system. It was the Working Group's consensus that RMO's must play a more active role in providing guidance to

Approved For Release 2007/07/10 : CIA-RDP86B00689R000300070005-6

Approved For Release 2007/07/10 : CIA-RDP86B00689R000300070005-6

data base managers. It is imperative, at minimum, that uniform standards for treating ADP information in lieu of paper as the Agency record be established. The Working Group's perception that new guidance from NARS on records management would not be forthcoming led to the proposal that the Agency undertake its own initiatives to establish guidelines for archival storage of ADP information.

c. Control, Storage and Archiving

To deal effectively with concerns such as data base duplication, the RMO function needs to be strengthened at the Directorate level. The Agency should follow the lead of the DDO in this arena. Machine-assisted policing of files for duplication would greatly assist all users.

At the individual level, employees must be educated to the legal need to purge and archive electronic holdings on their own. Procedures need to be set up so that "temporary" holdings will be periodically and automatically recalled and reviewed for disposition.

There was no Working Group sentiment or support for a single, monolithic archival system. This functionality is best served by satisfying the individual needs of the user community.

Likewise, there was little enthusiasm for an Agency-level data base administrator, nor was a hierarchy of such administrators recommended. To establish such may do little more than create an extra layer of bureaucracy, and a probable impediment to progress.

d. Data Definition Standards

Approved For Release 2007/07/10 : CIA-RDP86B00689R000300070005-6

Approved For Release 2007/07/10 : CIA-RDP86B00689R000300070005-6

It was consensus of the Group that some need to standardize on data definitions existed. However, the front-end investment required to make the numerous data bases and files compatible would almost be prohibitive. Further study in this area to examine the tradeoffs on standardizing versus unique data definitions is required. One mode of thought is that need will drive the effort to standardize on a case-by-case basis. Nevertheless, the Group recommended that a modest standardization effort be undertaken on an intra-Agency basis and that this effort focus on areas of real need for common access and interoperability.

e. Goals and Objectives

To insure optimum management of our information, the Working Group submits the following goal as a statement of Agency efforts in planning for an Information Handling Systems Architecture:

> Develop current and effective guidance for electronic records management. Implement an orchestrated program for controlling electronic data storage within the Agency and assuring that electronic records management is prudently enforced.

In pursuit of this goal, the following objectives are proposed:

Objective 2.1: Develop Records Management Policies for the electronic environment applicable to the Agency.

Objective 2.2: Strengthen the role of the RMO at the Directorate level and provide a means of educating employees in the art of data base management (with emphasis on purging and

Approved For Release 2007/07/10 : CIA-RDP86B00689R000300070005-6

Approved For Release 2007/07/10 : CIA-RDP86B00689R000300070005-6

cleaning up files).

Objective 2.3: Investigate implementation of a modest intra-Agency effort towards data standardization focused on areas of real, as opposed to abstract, needs for common access.

Approved For Release 2007/07/10 : CIA-RDP86B00689R000300070005-6